UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,177	11/05/2003	Jiwu Jing	9896-000013	7521

27572 7590 10/17/2007
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
10/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/702,177	**Applicant(s)** JING ET AL.	
	Examiner James Turchen	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 10 August 2007.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 19-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) 19-36 is/are allowed.

6)☒ Claim(s) 37-40 is/are rejected.

7)☒ Claim(s) 40 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 19-40 are pending. Claims 19-40 are new.

Response to Arguments

Applicant's arguments with respect to claims 19-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claim 40 is objected to because of the following informalities: “HSAH value” is listed within the claim when it seems as if applicant intends to use “HASH value”. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano (US 7,088,822).

Regarding claim 37:

Asano discloses:

splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the private key is constructed by one second sub-secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-keys according to an equation combination representation, and the number t is a positive integer [*figure 11, column 20 lines 4-20, column 21 lines 25-50; starting at KR, each level of tree corresponds to a level of the sub-secret keys; the first sub-secret keys corresponds to the parent node and each child (second sub-secret key) has all of the keys of its parent nodes; applicant does not specify within the claim what is intended by equation combination representation so examiner interprets as any function that modifies its inputs to achieve an output; although Asano does not disclose the use of private keys within the key tree, public/private key pairs are well known in the art and could have been used in the key tree*];

calculating t first calculation results according to the certificate to be signed and the t first sub-secret-keys in the multiple first sub-secret-keys upon receiving a certificate to be signed [*figure 12a and column 21 lines 25-50, the keys are encrypted with the parent keys, therefore the calculation results are the multiple decryptions required to obtain the key; column 5 lines 48-59, discloses the use of certificates, it is well known in the art that the certificates are signed with the private key corresponding to the public key of the certificate*];

obtaining the second sub-secret key corresponding to the t first sub-secret keys according to the equation combination representation [*figure 12a and column 21 lines 25-50, the key obtained from the calculation result is a sub-secret key*];

calculating a second calculation result according to the second sub-secret-key obtained and the certificate to be signed [*figure 12a and column 21 lines 25-50, the next sub-secret-key is obtained in the tree*] resulting in a second calculation result;

generating a digital signature according to the t first calculation results and the second calculation result [*it is well known in the art that a key is used in generating a digital signature*];

generating a digital certificate according to the digital signature and contents of the certificate to be signed [*it is well known in the art of certificate generation that a digital signature and the contents to go in the certificate are put into the certificate and signed by the private key*].

Regarding claim 38:

Asano discloses the method of claim 37, wherein the multiple first sub-secret-keys comprises multiple different random numbers [*it is well known that keys and sub-secret-keys must comprise random numbers, letters, or symbols or a mixture of the few*].

Claim 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yung et al. as applied to claim 37 above, and further in view of Yung et al. hereafter Yung (US 2002/0076052).

Regarding claim 39:

Asano discloses the method of claim 37, but does not disclose wherein the private key is a private key of RSA algorithm, and the private key is equal to the sum of t first sub-secret-keys and one second-subsecret-key. Yung discloses use of the RSA function [*paragraph 43*] for secure systems and the private key is a sum of sub-secret-keys [*paragraphs 63-66*]. It would have been obvious to combine the method of Asano with the method of Yung in order to allow end-to-end security by non-communicating hardware components within the high-end secure system [*paragraph 35*].

Regarding claim 40:

Asano discloses the method of claim 37, but does not disclose calculating hash value M by calculating a modular exponentiation of the hash value M and t first calculation results. Yung discloses use of the RSA algorithm in paragraph 43. Signing using the RSA algorithm comprise producing a hash value of the message and raising it to the power of d mod n and attaching that value as a signature. Yung also discloses generating a digital signature using modular multiplication [*paragraphs 63*-66]. It would have been obvious to one of ordinary to combine the method of Asano with the method of Yung in order to allow end-to-end security by non-communicating hardware components.

Allowable Subject Matter

Claims 19-36 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: Examiner is unable to find prior art that teaches "each equation combination representation comprises t items of j and I, j is sequence number of the secret share calcualator and i is number of the first sub-secret-key in the j-th secret share calculator, and each of j in one equation combination representation is different".

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

CHRISTOPHER REVAK
PRIMARY EXAMINER